PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-090039
(43)Date of publication of application : 31.03.2000

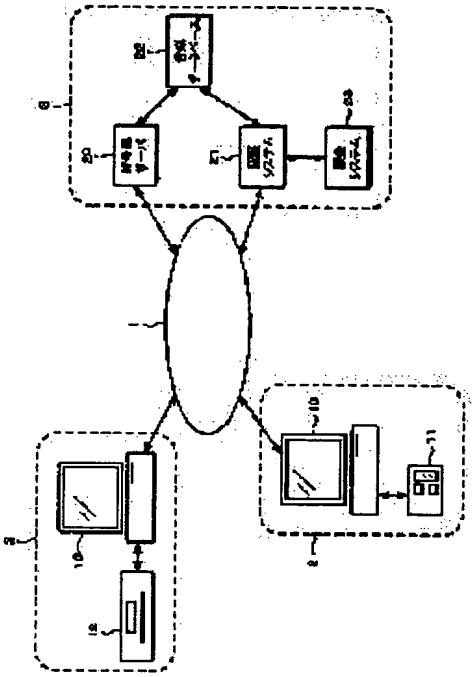
(51)Int.Cl. G06F 13/00
H04M 11/08
// G10K 15/04

(21)Application number : 10-260132
(22)Date of filing : 14.09.1998

(71)Applicant : SONY CORP
(72)Inventor : BIZEN NAOTO

(54) MUSIC DISTRIBUTING METHOD, TRANSMITTING DEVICE AND METHOD AND REPRODUCING DEVICE AND METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To sufficiently consider the protection of the copyright of distributed music data in a system distributing music data.
SOLUTION: A music server 3 and clients 2 are connected to the Internet 1. In the clients 2, a public key and a secret key are produced based on an ID proper to a reproducing device 11. The public key is sent to the server 3 to be registered and the secret key is held by the device 11. A client 2 requests the server 3 to distribute music data. Music data extracted from a music DB 22 is enciphered with the registered public key. The enciphered music data are transmitted to the client 2 and are stored in the reproducing device 11. At the time of reproducing them, the music data are reproduced while being decoded with the secret key held by the device 11. The music data stored in the device 11 can not be reproduced by other reproducing devices because they are enciphered with the key produced based on the ID proper to the device 11.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－90039
（P2000－90039A）
(43)公開日　平成12年３月31日(2000.3.31)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　13/00	３５４	Ｇ０６Ｆ　13/00	３５４Ｚ	５Ｂ０８９
Ｈ０４Ｍ　11/08		Ｈ０４Ｍ　11/08		５Ｄ１０８
// Ｇ１０Ｋ　15/04	３０２	Ｇ１０Ｋ　15/04	３０２Ｄ	５Ｋ１０１

審査請求　未請求　請求項の数11　ＯＬ　（全 16 頁）

(21)出願番号　特願平10－260132

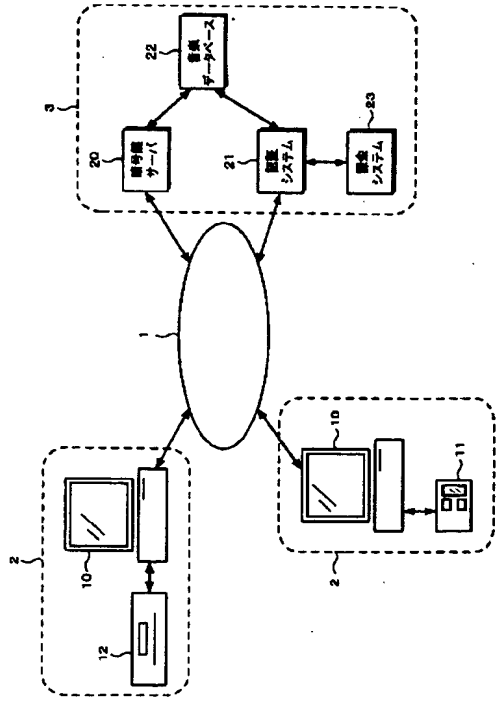
(22)出願日　平成10年９月14日(1998.9.14)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　尾前　尚登
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082762
弁理士　杉浦　正知

最終頁に続く

(54)【発明の名称】　音楽配信方法、送信装置および方法、ならびに、再生装置および方法

(57)【要約】
【課題】　音楽データを配信するシステムにおいて、配信された音楽データの著作権の保護を十分に配慮する。
【解決手段】　音楽サーバ３とクライアント２とがインターネット１に接続される。クライアント２において、再生装置１１固有のＩＤに基づき公開鍵及び秘密鍵が作成される。公開鍵は、サーバ３に送られ登録され、秘密鍵は、装置１１に保持される。クライアント２からサーバ３に対して、音楽データの配信が要求される。音楽ＤＢ２２から取り出された音楽データに対して、登録された公開鍵で暗号化が施される。暗号化された音楽データがクライアント２に送信され、再生装置１１に保存される。再生時には、装置１１に保持された秘密鍵で音楽データが復号化されながら再生される。装置１１に保存された音楽データは、装置１１固有のＩＤに基づき作成された鍵で暗号化されているため、他の再生装置では再生できない。



【特許請求の範囲】
【請求項１】　端末装置から要求された音楽データを、端末装置に対して配信する音楽配信方法において、
端末装置からの音楽データ配信の要求を受け付ける第１のステップと、
上記要求に基づき上記音楽データを上記端末装置に対して配信する第２のステップと、
上記要求があった上記端末装置の識別情報と、上記要求された上記音楽データとを関連付ける管理情報を蓄積する第３のステップと、
上記要求に基づき課金処理を行う第４のステップとを有し、
上記第１のステップで端末装置から音楽データ配信の要求を受け付けたときに、上記第３のステップでの上記管理情報に基づき、該端末装置による該音楽データ配信に対して上記第４のステップでの上記課金処理による課金が既に行われていると判断された場合、上記第４のステップで、課金をしないように処理するようにしたことを特徴とする音楽配信方法。
【請求項２】　端末装置から要求された音楽データを、端末装置に対して配信する送信装置において、
音楽データを保存する音楽データ保存手段と、
端末装置からの音楽データ配信の要求を受信する受信手段と、
上記受信手段によって受信された要求に基づき上記音楽データ保存手段から音楽データを出力する音楽データ出力手段と、
上記音楽データ出力手段によって出力された上記音楽データに対して暗号化を施す暗号化手段と、
上記暗号化された上記音楽データを上記端末に対して送信する送信手段とを有することを特徴とする送信装置。
【請求項３】　請求項２に記載の送信装置において、
端末装置で秘密鍵と共に作成された公開鍵を受信する鍵受信手段と、
上記鍵受信手段で受信された上記公開鍵と、該公開鍵を作成した端末装置情報とを管理する鍵管理手段とをさらに有し、
上記暗号化手段は、上記鍵管理手段の管理情報に基づき、上記要求のあった上記端末装置に対応した上記公開鍵によって上記音楽データに対する上記暗号化を施すことを特徴とする送信装置。
【請求項４】　請求項２に記載の送信装置において、
上記音楽データ保存手段では、音楽データは、圧縮符号化されて上記保存されていることを特徴とする送信装置。
【請求項５】　記憶媒体に記憶されたディジタルオーディオデータからなる音楽データを再生する再生装置において、
他の再生装置と区別するための識別情報を保持する識別情報保持手段と、
暗号化された音楽データが記憶される音楽データ記憶手段と、
再生時に、上記音楽データ記憶手段に記憶されている音楽データを読み出し、上記暗号を復号化する復号化手段と、
上記復号化手段から出力された音楽データをアナログ変換して音声信号として出力する音声信号出力手段とを有することを特徴とする再生装置。
【請求項６】　請求項５に記載の再生装置において、
上記復号化手段は、上記音楽データ記憶手段に記憶されている音楽データを読み出しながら、上記復号化を行うことを特徴とする再生装置。
【請求項７】　請求項５に記載の再生装置において、
上記識別情報に基づき公開鍵と共に作成された秘密鍵を保存する秘密鍵保存手段をさらに有し、
上記復号化手段は、上記鍵保存手段に保存された上記秘密鍵によって上記暗号の上記復号化を行うことを特徴とする再生装置。
【請求項８】　請求項５に記載の再生装置において、
上記記憶手段は、半導体メモリからなることを特徴とする再生装置。
【請求項９】　端末装置から要求された音楽データを、端末装置に対して配信する送信方法において、
音楽データを保存する音楽データ保存のステップと、
端末装置からの音楽データ配信の要求を受信する受信のステップと、
上記受信のステップによって受信された要求に基づき上記音楽データ保存のステップで保存された音楽データを出力する音楽データ出力のステップと、
上記音楽データ出力のステップによって出力された上記音楽データに対して暗号化を施す暗号化のステップと、
上記暗号化された上記音楽データを上記端末に対して送信する送信のステップとを有することを特徴とする送信方法。
【請求項１０】　記憶媒体に記憶されたディジタルオーディオデータからなる音楽データを再生する再生方法において、
他の再生装置と区別するための識別情報を保持する識別情報保持のステップと、
暗号化された音楽データが記憶される音楽データ記憶のステップと、
再生時に、上記音楽データ記憶のステップに記憶されている音楽データを読み出し、上記暗号を復号化する復号化のステップと、
上記復号化のステップから出力された音楽データをアナログ変換して音声信号として出力する音声信号出力のステップとを有することを特徴とする再生方法。
【請求項１１】　端末装置からサーバに対して音楽データの配信が要求され、該要求に基づきサーバから端末装置に対して音楽データの配信を行う音楽配信方法におい

て、
端末装置からサーバに対して音楽データ配信を要求する音楽データ配信要求のステップと、
上記音楽データ配信要求のステップで要求された該音楽データが該端末装置に対して既に配信したことがあるかどうかが調べられ、その結果に基づき、新規の要求であるとされれば課金を行い、過去に配信したことがあると判断されれば上記課金を行わない課金処理のステップと、
上記音楽データ配信要求のステップで要求された上記音楽データに対して、予め作成された、上記端末装置に固有の第１の鍵で暗号化を施す暗号化のステップと、
上記暗号化された上記音楽データを上記端末装置に送信する送信のステップと、
上記送信のステップで送信された上記音楽データを受信し、記憶媒体に記憶する記憶のステップと、
再生時に、上記記憶媒体から上記音楽データを読み出し、上記読み出された音楽データに施されている上記暗号を、予め作成された上記端末装置に固有の第２の鍵で、上記読み出しに伴い復号化する復号化のステップと、
上記復号化された音楽データをアナログ変換して音声信号として出力する音声信号出力のステップとを有することを特徴とする音楽配信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、著作権に配慮しつつ、ユーザが無駄なく音楽配信を利用することができるような音楽配信方法、送信装置および方法、ならびに、再生装置および方法に関する。
【０００２】
【従来の技術】現在、インターネットなどのネットワークや、衛星を用いたデータ通信の発達に伴い、多数の音楽データを蓄積した音楽配信サーバから、ユーザに対して音楽データの配信を行うサービスが出現しつつある。
【０００３】この音楽配信システムの一例として、音楽配信サーバには、例えばディジタルオーディオデータからなる音楽データが所定の方式で以て圧縮符号化され、多数蓄積される。ユーザは、パーソナルコンピュータなどを用いて、例えばインターネットを介して音楽配信サーバと接続し、音楽配信サーバに蓄積されている音楽データの中から所望の音楽データを選択し、ダウンロードを要求する。音楽配信サーバは、このダウンロード要求に基づき音楽データを検索し、そのデータをユーザ側に転送する。ユーザ側では、転送された音楽データを例えばパーソナルコンピュータのハードディスクに保存し、必要に応じて所定の再生手段によって再生する。
【０００４】
【発明が解決しようとする課題】このような音楽配信システムでは、通常、ユーザが音楽配信サーバから音楽データをダウンロードする際に課金が発生する。すなわち、例えば１音楽データ、あるいは、１回のダウンロードに付き所定の金額を音楽配信サーバ側に支払うことで、ユーザはダウンロードを許可され、所望の音楽データを入手することができる。従来では、このようなシステムに関し、同一のユーザが過去に課金されダウンロードした音楽データを再度ダウンロードする際にも、再び課金がなされてしまうという問題点があった。
【０００５】また、音楽データは、ディジタルデータとして配信される。そして、配信された音楽データは、上述したように、ユーザによって、ディジタルデータとして保存される。ディジタルデータは、周知のように、劣化無く何度でも複製が可能である。そのため、従来では、ダウンロードされた音楽データの著作権を保護することが非常に難しいという問題点があった。
【０００６】さらに、この問題に対処するために、音楽データを所定の暗号化方式で以て暗号化し、ユーザは、音楽配信サーバ側から予め与えられた鍵で、暗号化された音楽データを復号化する方法も考えられる。しかしながら、この方法でも、何らかの方法で暗号化された音楽データの鍵が破られてしまった場合、対処する方法が無いという問題点があった。
【０００７】したがって、この発明の目的は、ユーザに対して２重に課金するようなことが無いような音楽配信方法、送信装置および方法、ならびに、再生装置および方法を提供することにある。
【０００８】また、この発明の別の目的は、音楽データの著作権の保護に対して十分な配慮がなされた音楽配信方法、送信装置および方法、ならびに、再生装置および方法を提供することにある。
【０００９】また、この発明のさらに別の目的は、音楽データのセキュリティに対して十分な配慮がなされた音楽配信方法、送信装置および方法、ならびに、再生装置および方法を提供することにある。
【００１０】
【課題を解決するための手段】この発明は、上述した課題を解決するために、端末装置から要求された音楽データを、端末装置に対して配信する音楽配信方法において、端末装置からの音楽データ配信の要求を受け付ける第１のステップと、要求に基づき音楽データを端末装置に対して配信する第２のステップと、要求があった端末装置の識別情報と、要求された音楽データとを関連付ける管理情報を蓄積する第３のステップと、要求に基づき課金処理を行う第４のステップとを有し、第１のステップで端末装置から音楽データ配信の要求を受け付けたときに、第３のステップでの管理情報に基づき、端末装置による音楽データ配信に対して第４のステップでの課金処理による課金が過去に行われていると判断された場合、第４のステップで、課金をしないように処理するようにしたことを特徴とする音楽配信方法である。

【００１１】また、この発明は、端末装置から要求された音楽データを、端末装置に対して配信する送信装置において、音楽データを保存する音楽データ保存手段と、端末装置からの音楽データ配信の要求を受信する受信手段と、受信手段によって受信された要求に基づき音楽データ保存手段から音楽データを出力する音楽データ出力手段と、音楽データ出力手段によって出力された音楽データに対して暗号化を施す暗号化手段と、暗号化された音楽データを端末に対して送信する送信手段とを有することを特徴とする送信装置である。

【００１２】また、この発明は、記憶媒体に記憶されたディジタルオーディオデータからなる音楽データを再生する再生装置において、他の再生装置と区別するための識別情報を保持する識別情報保持手段と、暗号化された音楽データが記憶される音楽データ記憶手段と、音楽データ記憶手段に記憶されている音楽データを読み出し、暗号を復号化する復号化手段と、復号化手段から出力された音楽データをアナログ変換して音声信号として出力する音声信号出力手段とを有することを特徴とする再生装置である。

【００１３】また、この発明は、端末装置から要求された音楽データを、端末装置に対して配信する送信方法において、音楽データを保存する音楽データ保存のステップと、端末装置からの音楽データ配信の要求を受信する受信のステップと、受信のステップによって受信された要求に基づき音楽データ保存のステップで保存された音楽データを出力する音楽データ出力のステップと、音楽データ出力のステップによって出力された音楽データに対して暗号化を施す暗号化のステップと、暗号化された音楽データを端末に対して送信する送信のステップとを有することを特徴とする送信方法である。

【００１４】また、この発明は、記憶媒体に記憶されたディジタルオーディオデータからなる音楽データを再生する再生方法において、他の再生装置と区別するための識別情報を保持する識別情報保持のステップと、暗号化された音楽データが記憶される音楽データ記憶のステップと、音楽データ記憶のステップに記憶されている音楽データを読み出し、暗号を復号化する復号化のステップと、復号化のステップから出力された音楽データをアナログ変換して音声信号として出力する音声信号出力のステップとを有することを特徴とする再生方法である。

【００１５】また、この発明は、端末装置からサーバに対して音楽データの配信が要求され、要求に基づきサーバから端末装置に対して音楽データの配信を行う音楽配信方法において、端末装置からサーバに対して音楽データ配信を要求する音楽データ配信要求のステップと、音楽データ配信要求のステップで要求された音楽データが端末装置に対して過去に配信したことがあるかどうかが調べられ、その結果に基づき、新規の要求であるとされれば課金を行い、過去に配信したことがあるとされれば課金を行わない課金処理のステップと、音楽データ配信要求のステップで要求された音楽データに対して、予め作成された、端末装置に固有の第１の鍵で暗号化を施す暗号化のステップと、暗号化された音楽データを端末装置に送信する送信のステップと、送信のステップで送信された音楽データを受信し、記憶媒体に記憶する記憶のステップと、記憶媒体から音楽データを読み出し、読み出された音楽データに施されている暗号を、予め作成された端末装置に固有の第２の鍵で、読み出しに伴い復号化する復号化のステップと、復号化された音楽データをアナログ変換して音声信号として出力する音声信号出力のステップとを有することを特徴とする音楽配信方法である。

【００１６】上述したように、請求項１に記載の音楽配信方法によれば、音楽データの配信要求があった端末装置と既になされた課金処理とが関連付けられた管理情報に基づき、今回配信が要求された音楽データに対して既に課金されていれば、今回は課金されないように課金処理がなされるため、同一の音楽データに対して重複して課金されることがない。

【００１７】また、請求項２または９に記載の送信装置または方法によれば、配信を要求された音楽データを、暗号化を施して送信するため、送信された音楽データの著作権が保護される。

【００１８】また、請求項５または１０に記載の再生装置または方法によれば、他の再生装置と区別するための識別情報が保持されると共に、暗号化が施されたまま記憶媒体に記憶された音楽データを、記憶媒体から読み出しながら暗号の復号化を行い、復号化された音楽データをアナログ変換して音声信号として再生するため、記憶媒体に記憶されている音楽データの著作権が保護される。

【００１９】また、請求項１１記載の音楽配信方法によれば、端末装置からサーバに対して音楽データの配信が要求され、要求された音楽データがその端末装置に対して既に配信したことがあれば課金が行われず、新規に要求されたものであれば課金が行われると共に、音楽データは、予め作成された、端末装置に固有の第１の鍵で暗号化されて端末装置に対して送信され、送信された音楽データを受信した端末装置では、受信された音楽データが記憶媒体に記憶され、再生時に記憶媒体から読み出された音楽データに対して、予め作成された、端末装置に固有の第２の鍵で暗号の復号化が行われるため、同一の音楽データの配信要求に対して重複して課金がなされないと共に、音楽データが端末装置に固有の鍵で暗号化／復号化されるため、音楽データの著作権が保護される。

【００２０】

【発明の実施の形態】以下、この発明の実施の一形態を、図面を参照しながら説明する。図１は、この発明に適用できる音楽配信システムの構成の一例を示す。例え

ばインターネットであるネットワーク１に対して、音楽データの配信を受ける側であるクライアント２が多数、接続される。また、ネットワーク１に対して、音楽データの配信を行う側である音楽配信サーバ３が接続される。

【００２１】この例では、ユーザすなわちクライアント２と音楽配信サーバ３との間で、特定の契約が交わされることによって、音楽配信サーバ３からクライアント２に対する音楽データの配信を行うことができるようになる。契約されたクライアント２から音楽配信サーバ３に対して、ネットワーク１を介して音楽データのダウンロードが要求される。音楽配信サーバ３は、この要求に基づき、音楽データを、ネットワーク１を介して要求のあったクライアント２に対して送信し、音楽データの配信を行う。

【００２２】音楽データは、暗号化されて配信される。クライアント２では、配信された音楽データを暗号化されたまま保存する。暗号化の方式としては、例えば公開鍵方式を用いることができる。これは、周知のように、暗号化のための鍵である公開鍵と、暗号を解読するための鍵である秘密鍵との、２つの鍵を用いる方式である。２つの鍵は、暗号を送られる側で作成される。公開鍵は、暗号化を行う側に送られ、秘密鍵は暗号を送られる側で保存される。公開鍵で作成された暗号は、対応する秘密鍵でしか解読できない。

【００２３】クライアント２は、この音楽配信システムの端末装置として構成され、例えばパーソナルコンピュータ１０と、パーソナルコンピュータ１０と所定のインターフェイスによって接続可能な携帯用オーディオ再生装置１１とからなる。携帯用オーディオ再生装置１１の代わりに、据置型オーディオ再生装置１２を備えてもよい。これら再生装置１１および１２は、オーディオデータの記録の機能を有していてもよい。

【００２４】音楽配信サーバ３は、複数のサーバからなるシステムである。音楽配信サーバ３は、暗号鍵サーバ２０，認証システム２１，音楽データベース２２および課金システム２３を有する。

【００２５】暗号鍵サーバ２０は、公開鍵の管理などを行うと共に、配信される音楽データの暗号化を行う。音楽データベース２２には、ディジタルオーディオデータからなる音楽データが多数、蓄積されており、ユーザからの音楽データの配信要求に基づき、音楽データの検索を行う。認証システム２１は、ユーザに関する情報が管理されたユーザデータベースを有し、ユーザ情報が蓄積されると共に、音楽データの配信を要求してきたユーザが正規のユーザであるかどうかの認証を行う。また、課金システム２３は、音楽データの配信を要求してきたユーザのうち、課金を行うべきユーザに対して課金処理を行う。これらのサーバならびにシステム間では、互いに情報の参照を行うことができる。

【００２６】なお、音楽データベース２２に蓄積されている音楽データは、所定の方式で圧縮符号化される。これは、圧縮符号化されて音楽データベース２２に蓄積されるようにしてもよいし、音楽データベース２２から出力されてから圧縮符号化するようにしてもよい。圧縮符号化の方式としては、ＡＴＲＡＣ(Adaptive TranformAcoustic Coding：商標）、ＡＴＲＡＣが改良されたＡＴＲＡＣ２（商標）、ＭＰＥＧ(Moving Picture Experts Group)オーディオ、ＴｗｉｎＶＱ（商標）など、様々な方式を用いることができる。

【００２７】クライアント２から音楽配信サーバ３に対して、ネットワーク１を介して音楽データの配信が要求される。このとき、予めユーザに与えられた認証用ＩＤが音楽配信サーバ３に対して送信される。この認証用ＩＤが認証システム２１で確認され、正規のユーザからの要求であるとされると、音楽データベース２２に対して要求された音楽データの検索が指示されると共に、課金システム２３に対して、そのユーザに対する課金処理を行う指示が出される。検索された音楽データは、暗号鍵サーバ２０で、予め認証サーバ２１に登録されている、クライアント２の公開鍵で以て暗号化され、ネットワーク１を介して要求を出したクライアント２に対して送信される。

【００２８】クライアント２では、音楽配信サーバ３から配信された音楽データは、暗号化されたまま、例えば一旦パーソナルコンピュータ１０に保存され、音楽データのダウンロードがなされる。そして、音楽データは、暗号化されたまま携帯用オーディオ再生装置１１に転送される。携帯用オーディオ再生装置１１は、使用時にはパーソナルコンピュータ１０と切り離して用いられ、パーソナルコンピュータ１０から転送された音楽データの再生がなされる。音楽データは、携帯用オーディオ再生装置１１において、上述の公開鍵と共に予め作成された秘密鍵で以て、暗号化を解かれながら再生される。

【００２９】なお、課金は、例えば図示されない専用の回線により課金システム２３クライアント２とが接続され、月毎などの単位で集計され、所定の金融機関から引き落とすようにされる。これに限らず、例えばプリペイドカードを利用しその都度支払うようにしてもよい。

【００３０】また、図１の構成は、この例に限定されない。例えば、ネットワーク１の代わりに、衛星を利用した通信システムを用いることができる。この場合、クライアント２と音楽配信サーバ３とは、所定の回線、例えば公衆電話回線で接続される。この回線を通じて、クライアント２から音楽配信サーバ３に対して音楽データの配信要求が出される。音楽配信システム３では、この要求に基づき音楽データベース２２が検索され、衛星を介してクライアント２に対して音楽データの配信が行われる。

【００３１】図２は、携帯用オーディオ再生装置１１の

構成の一例を示す。この例では、再生装置１１は、音楽データの記録媒体として半導体メモリを用いた携帯用ヘッドフォンステレオ１１である。Ｆ－ＲＯＭ３０は、音楽データを記憶するためのフラッシュメモリである。Ｆ－ＲＯＭ３０は、電気的に内容の消去を行い、データを書き替えることができる。Ｆ－ＲＯＭ３０は、メモリコントローラ３１によって、データの読み出しや書き替えの制御が行われる。例えば、外部インターフェイス３９から供給された音楽データは、メモリコントローラ３１の制御によってＦ－ＲＯＭ３０に書き込まれる。

【００３２】なお、メモリコントローラ３１は、後述するシスコン３６の制御に基づき、Ｆ－ＲＯＭ３０から読み出された音楽データを、秘密鍵を用いて復号化する機能を有する。この復号化の処理は、音楽データの読み出しに伴い、リアルタイムで行われる。

【００３３】メモリコントローラ３１の制御によってＦ－ＲＯＭ３０から音楽データが読み出され、暗号の復号化がなされ、デコーダ３２に供給される。音楽データは、所定の方式、例えばＡＴＲＡＣ２方式で以て圧縮符号化されている。このデコーダ３２で、この圧縮符号化が解かれディジタルオーディオデータとされた音楽データは、ＤＳＰ３３に供給される。

【００３４】ＤＳＰ３３は、後述するシスコン３６からのコマンドにより、供給されたディジタルオーディオデータに対して所定の処理、例えばイコライジング処理やレベル調整処理などを施す。ＤＳＰ３３から出力されたディジタルオーディオデータは、図示されないＤ／Ａ変換器によってアナログオーディオ信号に変換され、アナログアンプ３４に供給される。そして、所定のレベルまで増幅され、例えばヘッドフォン３５に供給され、再生音声とされる。

【００３５】外部インターフェイス３９は、Ｆ－ＲＯＭ３０に対して音楽データの転送を行う際に用いられるインターフェイスである。外部インターフェイス３９と後述するパーソナルコンピュータ１０の対応するインターフェイスとが所定のケーブルで接続され、パーソナルコンピュータ１０からこの携帯用ヘッドフォンステレオ１１に対して音楽データなどの転送が行われる。なお、インターフェイスはこれに限らず、例えば赤外線信号を利用したワイヤレスのものを用いることもできる。

【００３６】シスコン３６は、ＣＰＵ，ＲＯＭおよびＲＡＭなどを有し、この携帯用ヘッドフォンステレオ１１の全体を制御する。ＲＯＭには、初期プログラムやこの携帯用ヘッドフォンステレオ１１のシリアル番号などが予め記憶される。ＲＯＭには、書き替え可能なフラッシュＲＯＭを用いるようにできる。また、ＲＡＭは、ＣＰＵが動作するためのワークメモリである。シスコン３６によって、上述したメモリコントローラ３１，デコーダ３２およびＤＳＰ３３が制御される。

【００３７】操作部３７は、ユーザの操作に基づきシスコン３６に対して制御信号を供給する。また、表示部３８は、例えば液晶ディスプレイ（ＬＣＤ）であり、シスコン３６から供給される表示信号に基づく表示を行う。

【００３８】例えば、Ｆ－ＲＯＭ３０に書き込まれている音楽データの曲名リストが表示部３８に表示される。ユーザは、この表示に基づき操作部３７を操作し、所望の音楽データの再生を指示する。この指示に基づく制御信号がシスコン３６に供給される。この制御信号によってシスコン３６によってメモリコントローラ３１が制御され、Ｆ－ＲＯＭ３０から該当する音楽データが読み出される。読み出された音楽データは、メモリコントローラ３１，デコーダ３２，ＤＳＰ３３およびアナログアンプ３４でそれぞれ所定の処理をされ、ヘッドフォン３５で再生される。

【００３９】図3は、パーソナルコンピュータ１０の構成の一例を示す。この例では、パーソナルコンピュータ１０は、一般的な構成を有し、例えばバス５０に対してＣＰＵ５１，ＲＡＭ５２およびＲＯＭ５３が接続されると共に、図示されないディスプレイアダプタを介してディスプレイ５４が接続される。ＲＡＭ５２は、ＣＰＵ５１のワークメモリであり、ＲＯＭ５３には、初期プログラムなどが予め記憶される。

【００４０】また、バス５０に対して、さらに、ハードディスクドライブ（ＨＤＤ）５５が接続されると共に、入出力インターフェイス５６が接続される。入出力インターフェイス５６は、このパーソナルコンピュータ１０外部とのデータのやり取りを司る。入出力インターフェイス５６には、例えばキーボード５８やマウス５９、フロッピーディスクやＭＯ(Magneto-Optical disc)などの着脱自在な記録媒体を用いる外部記憶装置６１、ネットワーク１や公衆電話回線などと通信を行うためのモデム５８が接続される。

【００４１】また、入出力インターフェイス５６には、上述した携帯用ヘッドフォンステレオ１１との通信を行うためのインターフェイス５７が接続される。すなわち、このインターフェイス５７と、上述の携帯用ヘッドフォンステレオ１１の外部インターフェイス３９とが所定のケーブルで接続される。これにより、パーソナルコンピュータ１０から携帯用ヘッドフォンステレオ１１に対する音楽データの転送が行われる。

【００４２】音楽配信サーバ3からネットワーク１を介して配信された音楽データは、モデム５８で受信され、入出力インターフェイス５６およびバス５０を介してＨＤＤ５５に一旦書き込まれる。音楽データは、ＨＤＤ５５から読み出され、バス５０および入出力インターフェイス５６とを介してインターフェイス５７に供給される。そして、インターフェイス５７から携帯用ヘッドフォンステレオ１１の外部インターフェイス３９に対して供給される。

【００４３】次に、この実施の一形態による、音楽デー

タのダウンロードの方法について説明する。図４は、ダウンロードの際の処理を概略的に示すフローチャートである。図４では、携帯用ヘッドフォンステレオ１１，パーソナルコンピュータ１０からなるクライアント２、および、音楽配信サーバ３のそれぞれの処理が互いに関連されて示されている。なお、以下の図中では、携帯用ヘッドフォンステレオは、携帯用ＨＳあるいは単にＨＳと省略されて示されている。

【００４４】先ず、この図４に示される処理の開始に先んじて、携帯用ヘッドフォンステレオ１１とパーソナルコンピュータ１０とが所定のインターフェイスによって接続され、互いに通信可能な状態とされる。そして、携帯用ヘッドフォンステレオ１１では、図４のステップＳ２１の「Ｎ」で示されるように、パーソナルコンピュータ１０との通信待ちの状態とされる。また、音楽配信サーバ３でも、パーソナルコンピュータ１０との通信待ち状態とされる（ステップＳ２５の「Ｎ」）。

【００４５】ユーザは、音楽配信サーバ３に対する音楽データのダウンロードの要求を、パーソナルコンピュータ１０に対して指示する。この指示が出されると、先ず、パーソナルコンピュータ１０から携帯用ヘッドフォンステレオ１１に対して、認証用ＩＤが要求される（ステップＳ１０）。そして、パーソナルコンピュータ１０は、携帯用ヘッドフォンステレオ１１からの認証用ＩＤの受信待ち状態とされる（ステップＳ１１の「Ｎ」）。

【００４６】パーソナルコンピュータ１０からの要求は、インターフェイス５７を介して携帯用ヘッドフォン１１に対して送信される。携帯用ヘッドフォン１１では、この要求が外部インターフェイス３９およびメモリコントローラ３１を介してシスコン３６に供給される。そして、受け取ったこの要求に基づき、パーソナルコンピュータ１０に対して認証用ＩＤを送信する（ステップＳ２２）。

【００４７】認証用ＩＤは、例えば、この携帯用ヘッドフォンステレオ１１のそれぞれに対して予め与えられ、シスコン３６のＲＯＭに記憶された、ユニークなシリアル番号を用いることができる。この認証用ＩＤは、例えば、この携帯用ヘッドフォンステレオ１１の出荷時などに、認証用サーバ２１のユーザデータベースに対して予め登録しておくことができる。

【００４８】この認証用ＩＤがパーソナルコンピュータ１０に受信されたら（ステップＳ１１の「Ｙ」）、処理はステップＳ１２に移行し、パーソナルコンピュータ１０から音楽配信サーバ３に対して、認証用ＩＤに基づく認証の確認が要求される。そして、パーソナルコンピュータ１０は、音楽配信サーバ３からの認証結果待ちとされる（ステップＳ１３の「Ｎ」）。

【００４９】音楽配信サーバ３では、パーソナルコンピュータ１０からの認証の確認要求の送信を受けると（ステップＳ２５の「Ｙ」）、認証システム２１においてユーザデータベースが参照され、送られた認証用ＩＤの確認が行われる。認証結果は、パーソナルコンピュータ１０に送信される（ステップＳ２６）。

【００５０】認証結果が送信されると、音楽配信サーバ３側は、パーソナルコンピュータ１０からの音楽データのダウンロード要求待ちとされる（ステップＳ２７の「Ｎ」）。

【００５１】音楽配信サーバ３からの認証結果がパーソナルコンピュータ１０に受信されると（ステップＳ１３の「Ｙ」）、処理はステップＳ１４に移行し、認証結果の判定が行われる。そして、認証の結果、認証要求を送信したパーソナルコンピュータ１０が音楽データの配信を受けるのが不適切である（ＮＧ）と判断されると、処理はステップＳ１５に移行し、ユーザに対して理由が通知され、一連の処理が終了される。音楽データの配信を受けるのが不適切である理由としては、例えば、（１）認証用ＩＤが登録されているものではなく、そのユーザが正規ユーザではないと判断された場合、（２）複数の互いに異なるユーザから同一の認証用ＩＤが送信された場合、などが挙げられる。パーソナルコンピュータ１０のディスプレイ５４上に、これらの情報が表示される。

【００５２】なお、同一ユーザから互いに異なる複数の認証用ＩＤが送られてきた場合には、その認証用ＩＤでの使用を不可とすると良い。また、上述の（２）の例としては、ハードウェアをリバースエンジニアなどでまるごと不正コピーされた場合が考えられる。

【００５３】一方、ステップＳ１４で、認証の結果、認証要求を送信したパーソナルコンピュータ１０が音楽データの配信を受けるのが適切である（ＯＫ）であると判断されると、処理はステップＳ１６に移行し、パーソナルコンピュータ１０から音楽配信サーバ３に対して、音楽データのダウンロード要求が出される。

【００５４】例えば、音楽配信サーバ３が有する音楽データのリストに基づき、ユーザによって所望の音楽データが選択される。パーソナルコンピュータ１０に対して選択された音楽データを表す情報が入力され、音楽配信サーバ３に対する音楽データのダウンロード要求が出される。

【００５５】音楽データのリストは、音楽配信サーバ３側からユーザに対して配付される。ネットワーク１を介して、ユーザが音楽配信サーバ３から得られるようにしてもよい。これに限らず、パーソナルコンピュータ１１からネットワーク１を介して音楽データベース２２に対してアクセスし、所望の音楽データを検索するようにもできる。

【００５６】音楽配信サーバ３側では、ステップＳ２７にてパーソナルコンピュータ１０からの音楽データのダウンロード要求が受信される。そして、次のステップＳ２８で、音楽データベース２２に対して、ダウンロードが要求された音楽データの検索が行われる。検索された

音楽データは、ステップS29で、そのユーザから送られた公開鍵で以て暗号化され、パーソナルコンピュータ10に送信される。このステップS29での処理については後述するが、このときに、ユーザに対する課金処理も行われる。

【0057】なお、図示しないが、音楽データが送信される際、その旨がユーザ情報と対応付けられて認証システム21のユーザデータベースに格納される。ユーザから音楽データのダウンロード要求があった場合に、このユーザデータベースが参照され、過去にそのユーザに対して該当音楽データをダウンロードしたかどうか、また、そのときの課金情報が調べられる。これにより、同一のユーザが同一の音楽データをダウンロードする際に重複して課金されるのを防ぐことができる。

【0058】パーソナルコンピュータ10では、ステップS17のダウンロード待機状態にて、音楽配信サーバ3から送信された音楽データが受信され、音楽データのダウンロードがなされる。次のステップS18でダウンロードされた音楽データの保存先が指定される。この例では、音楽データの保存先を、パーソナルコンピュータ10のハードディスク55と、携帯用ヘッドフォンステレオ11とから選択して指定できる。パーソナルコンピュータ10のハードディスク55への保存を選択した場合は、処理はステップS19へ移行し、ダウンロードされた音楽データがハードディスク55に保存され、一連の処理が終了される。なお、音楽データは、暗号化されたまま、ハードディスク55に保存される。

【0059】一方、ステップS18で、音楽データの保存先を、携帯用ヘッドフォンステレオ11に選択した場合、処理はステップS20に移行する。そして、ダウンロードされた音楽データが携帯用ヘッドフォンステレオ11に転送される。

【0060】音楽データは、インターフェイス57を介して携帯用ヘッドフォンステレオ11に転送される。携帯用ヘッドフォンステレオ11側では、音楽データは、外部インターフェイス39から供給され（ステップS23）、メモリコントローラ31を介してF－ROM30に保存される（ステップS24）。この場合も、音楽データは、暗号化されたままF－ROM33に保存される。

【0061】次に、上述のステップS29での、音楽配信サーバ3における音楽データの暗号化ならびにパーソナルコンピュータ10への転送の処理について、図5のフローチャートを用いて説明する。ステップS291は、上述のサーバ3側の処理における、ステップS25～ステップS28の処理である。ステップS292で、ダウンロード要求された音楽データが同一ユーザによって既にダウンロードされたデータであるかどうかが判断される。これは、上述したように、認証システム21が有するユーザデータベースを参照することで判断される。

【0062】若し、今回ダウンロードを要求された音楽データがそのユーザによって過去にダウンロードされたことがあるものであると判断されたら、処理はステップS294に移行する。

【0063】一方、ステップS292で、今回ダウンロード要求が出された音楽データが、そのユーザによって過去にダウンロードされている音楽データではないとされたら、処理はステップS293に移行し、課金システム23によって課金処理が行われる。この課金処理によって、そのユーザに対して、所定金額を支払うような指示が出される。

【0064】そして、ステップS294で、ダウンロード要求された音楽データに対して、予めそのユーザから送られ、認証システム21に登録されている公開鍵による暗号化が施される。暗号化された音楽データは、次のステップS295で、パーソナルコンピュータ10に対して転送される。

【0065】次に、認証システム21に対して、新規に認証用IDを登録する際の手順の例について、図6のフローチャートを用いて説明する。なお、このフローチャートが実行されるのに先立って、携帯用ヘッドフォンステレオ11とパーソナルコンピュータ10とが所定のインターフェイスによって接続され、互いに通信可能な状態とされる。

【0066】先ず、ステップS30で、パーソナルコンピュータ10から携帯用ヘッドフォンステレオ11に対して認証用IDが要求される。携帯用ヘッドフォンステレオ11では、パーソナルコンピュータ10との通信待ちの状態（ステップS36の「N」）において、この要求が受信されると（ステップS36の「Y」）、次のステップS37で、パーソナルコンピュータ10に対して認証用IDが送信される。

【0067】パーソナルコンピュータ10では、認証用ID受信待ちの状態（ステップS31の「N」）においてこの認証用IDを受信すると、次のステップS32で、受信された認証用IDに基づき、公開鍵と秘密鍵とが作成される。作成された公開鍵は、認証システム21に送信される（ステップS33）。また、公開鍵と共に、そのユーザの認証用IDや、ユーザID、パスワードなども送られる。

【0068】音楽配信サーバ3側では、パーソナルコンピュータ10からの鍵の受信待ちの状態（ステップS40の「N」）において、この公開鍵が受信されると（ステップS40の「Y」）、処理は次のステップS41に移行する。ステップS41では、認証システム21で、受信された認証用IDのチェック、パスワードやユーザIDのチェックなどが行われる。そして、認証システム21のユーザデータベースに、受信された公開鍵が登録される。パーソナルコンピュータ10に送信される音楽

データは、登録された公開鍵を用いて暗号化される。

【００６９】一方、パーソナルコンピュータ１０では、ステップＳ３２で作成された秘密鍵が携帯用ヘッドフォンステレオ１１に対して転送される（ステップＳ３４）。携帯用ヘッドフォンステレオ１１では、秘密鍵の受信待ちの状態（ステップＳ３８の「Ｎ」）で、パーソナルコンピュータ１０から送られた秘密鍵を受け取ると（ステップＳ３８の「Ｙ」）、次のステップＳ３９で、受信された秘密鍵を保存する。秘密鍵は、例えばシスコン３６が有する、バッテリバックアップされたＲＡＭに保存される。シスコン３６のＲＯＭに書き込むようにしてもよい。これに限らず、Ｆ－ＲＯＭ３０の所定領域に保存されるようにしてもよい。

【００７０】次に、ダウンロードされた音楽データを、パーソナルコンピュータ１０から携帯用ヘッドフォンステレオ１１に転送し、再生する手順について、図７のフローチャートを用いて説明する。なお、この手順に先んじて、パーソナルコンピュータ１０に対して、ユーザが固有に有するユーザＩＤとパスワードとが予め入力され、例えばハードディスク５５の所定領域に記憶されているものとする。また、携帯用ヘッドフォンステレオ１１固有の認証用ＩＤがパーソナルコンピュータ１０に予め記憶されており、ユーザＩＤおよびパスワードと関連付けられる。

【００７１】図７のフローチャートにおいて、最初のステップＳ５０で、パーソナルコンピュータ１０から携帯用ヘッドフォンステレオ１１に対して認証用ＩＤが要求される。携帯用ヘッドフォンステレオ１１では、パーソナルコンピュータ１０との通信待ちの状態（ステップＳ５６の「Ｎ」）において、この要求が受信されると（ステップＳ５６の「Ｙ」）、次のステップＳ５７で、パーソナルコンピュータ１０に対して認証用ＩＤが送信される。

【００７２】パーソナルコンピュータ１０では、認証用ＩＤ受信待ちの状態（ステップＳ５１の「Ｎ」）においてこの認証用ＩＤを受信すると、次のステップＳ５２で、受信された認証用ＩＤがチェックされる。このとき、パーソナルコンピュータ１０上で、そのユーザに対して決められたユーザＩＤおよびパスワードの入力が要求される。チェックは、例えば、入力されたユーザＩＤおよびパスワードの組み合わせが判定されると共に、これらユーザＩＤおよびパスワードと、携帯用ヘッドフォンステレオ１１固有の認証用ＩＤとが互いに対応するかどうかを調べることでなされる。

【００７３】若し、これら認証用ＩＤとユーザＩＤおよびパスワードとが所定の関係になければ、チェックの結果がＮＧ(No Good) とされ、処理はステップＳ５５に移行する。そして、ステップＳ５５で、その理由がパーソナルコンピュータ１０のディスプレイ上に表示される。一例としては、「ユーザＩＤあるいはパスワードが間違っています」、「不正な認証用ＩＤです」などと表示される。

【００７４】一方、ステップＳ５２で、認証用ＩＤとユーザＩＤおよびパスワードとが所定の関係にあり、認証結果がＯＫであるとされれば、処理はステップＳ５３に移行する。そして、ユーザにより選曲がなされ、パーソナルコンピュータ１０から携帯用ヘッドフォンステレオ１１に対して転送する音楽データが選択される。ステップＳ５４で、選択された音楽データがヘッドフォンステレオ１１に対して転送される。上述したように、音楽データは、ハードディスク５５上に暗号化されたまま保存されている。ステップＳ５４での転送も、音楽データが暗号化されたまま、行われる。

【００７５】携帯用ヘッドフォンステレオ１１側では、パーソナルコンピュータ１０からの音楽データの転送待ちの状態（ステップＳ５８の「Ｎ」）において、この音楽データが受信されると（ステップＳ５８の「Ｙ」）、次のステップＳ５９で、受信された音楽データがＦ－ＲＯＭ３０に対して保存される。

【００７６】携帯用ヘッドフォンステレオ１１において、Ｆ－ＲＯＭ３０に保存された音楽データの再生がステップＳ６０で指示される。この指示により、Ｆ－ＲＯＭ３０に保存された音楽データがメモリコントローラ３１の制御に基づき読み出される。読み出された音楽データは、上述の図６のステップＳ３９で、予め携帯用ヘッドフォンステレオ１１に対して記憶された秘密鍵を用いて復号化されながら（ステップＳ６１）、デコーダ３２に供給される。

【００７７】なお、秘密鍵による音楽データの復号化は、この例では、ハードウェア的に処理される。例えば、暗号を解くためのアルゴリズムが内蔵された集積回路に対して、秘密鍵がパラメータとして与えられ、暗号化された音楽データの復号化がなされる。また、これに限らず、ハードウェアが十分な処理速度を有していれば、ソフトウェア的な処理で復号化を行ってもよい。

【００７８】音楽データは、デコーダ３２で、音楽配信サーバ３側で施された圧縮符号化が解かれ（ステップＳ６２）、ＤＳＰ３３に供給され所定の信号処理を施される。ＤＳＰ３３の出力は、図示しないＤ／Ａ変換器によってアナログオーディオ信号に変換され（ステップＳ６３）、アンプ３４で増幅されヘッドフォン３５で再生される。

【００７９】次に、この発明による、音楽データに対するセキュリティ、すなわち、著作権を保護するための機構について、図８を用いて説明する。クライアント２側では、携帯用ヘッドフォンステレオ１１における、例えばユニークなシリアル番号を認知用ＩＤとして、この認知用ＩＤに基づいて秘密鍵１０１および公開鍵１００を作成する。秘密鍵１０１は、携帯用ヘッドフォンステレオ１１に保存され、公開鍵１００は、サーバ３に送ら

れ、保存ならびに管理される。

【００８０】既に述べたように、音楽データは、サーバ３からクライアント２に対して転送される際に、転送するユーザから送られた公開鍵によって暗号化される。また、携帯用ヘッドフォンステレオ１１では、音楽データは、暗号化されたまま保存され、再生時に秘密鍵を用いて再生される。

【００８１】そのため、クライアント２側では、こうして転送された音楽データは、公開鍵１００と対応する秘密鍵１０１を有する携帯用ヘッドフォンステレオ１１でしか再生できない。例え、転送された音楽データをハードディスク５５に保存し、別の携帯用ヘッドフォンステレオ１１'（図示しない）で再生しようとしても、その携帯用ヘッドフォンステレオ１１'は、公開鍵１００に対応する秘密鍵１０１を有していないので、再生できない。したがって、音楽データを複製しても、複製された音楽データは、公開鍵１００に対応する秘密鍵１０１を持たない他の機器では再生できず、その音楽データの著作権が保護されることになる。

【００８２】また、何らかの方法で秘密鍵１０１が破られてしまった場合でも、対応が可能である。一例として、例えば悪意の第三者による秘密鍵の盗用などが行われた場合、その秘密鍵と対応する公開鍵をサーバ３側で消去すると共に、正規のユーザに対して、新しい認知用ＩＤを配付する。これは、例えば携帯用ヘッドフォンステレオ１１のファームウェアの書き替えを行い、シリアル番号を変更することでなされる。この新しい認知用ＩＤに基づき、新規に、公開鍵１００および秘密鍵１０１とを作成することで、盗用された秘密鍵を使用することができなくなる。

【００８３】なお、上述では、音楽データの暗号化に公開鍵方式を用いているが、これはこの例に限定されない。例えばＤＥＳ(Data Encryption Standard)方式といった、共通鍵方式を用いて音楽データの暗号化を行うようにしてもよい。この場合、共通鍵は、サーバ３からクライアント２へ、予め配付される。

【００８４】また、上述では、音楽データは、携帯用ヘッドフォンステレオ１１において再生時に復号化されるとしたが、これはこの例に限定されない。例えば、暗号化されたままＦ－ＲＯＭ３０に記憶された音楽データを、例えばバッファメモリなどを利用して予め復号化しておき、再びＦ－ＲＯＭ３０に書き戻すことも考えられる。

【００８５】さらに、上述では、クライアント２においてパーソナルコンピュータ１０を用いて端末装置が構成されているが、これはこの例に限定されない。他の情報機器、例えば衛星放送などを受信するためのセットトップボックスを、このパーソナルコンピュータ１０の代わりに用いることもできる。また、この音楽配信に専用の情報機器を設けることもできる。

【００８６】

【発明の効果】以上説明したように、この発明によれば、一度ダウンロードして課金された音楽データに対して、次回のダウンロードからは課金がなされない。そのため、ユーザは、連続再生するだけの容量を有したハードディスクなどの記録媒体を用意すればよいという効果がある。

【００８７】また、同じ音楽データに対して課金がなされないため、ユーザは、必要なときに音楽データのダウンロードを行うことができる。そのため、音楽データのバックアップなどを行う必要がないという効果がある。

【００８８】さらに、この発明では、音楽データは、暗号化されてダウンロードされると共に、暗号化されたままユーザの下に保存される。そして、音楽データの再生は、再生装置に固有の鍵で復号化されながら行われる。そのため、音楽データの著作権が十分保証されるという効果がある。

【００８９】さらにまた、この実施の一形態では、暗号化鍵が破られた場合にも対処可能であるという効果がある。

【図面の簡単な説明】

【図１】この発明に適用できる音楽配信システムの構成の一例を示す略線図である。

【図２】携帯用ヘッドフォンステレオの構成の一例を示すブロック図である。

【図３】パーソナルコンピュータの構成の一例を示すブロック図である。

【図４】音楽データのダウンロードの際の処理を概略的に示すフローチャートである。

【図５】音楽データの暗号化ならびにパーソナルコンピュータへの転送の処理を説明するためのフローチャートである。

【図６】認証システムに対して新規に認証用ＩＤを登録する際の手順の一例を説明するためのフローチャートである。

【図７】ダウンロードされた音楽データをパーソナルコンピュータから携帯用ヘッドフォンステレオに転送し再生する手順を説明するためのフローチャートである。

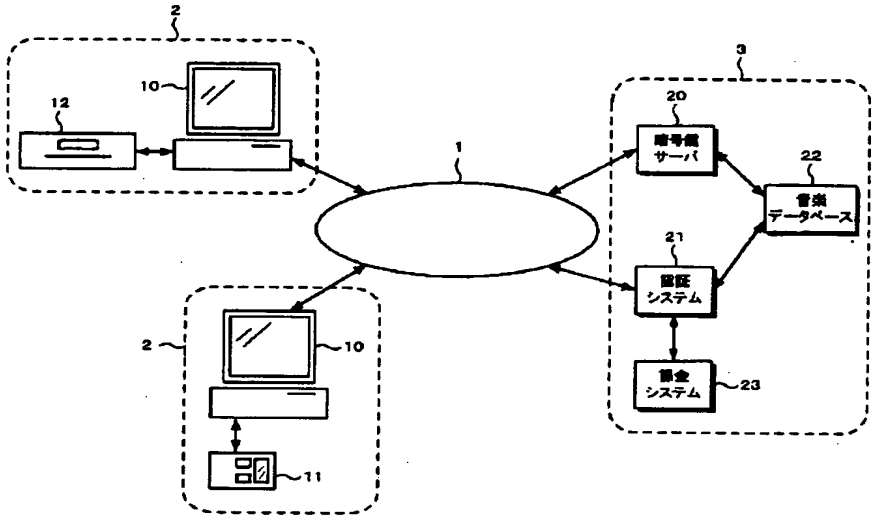
【図８】音楽データの著作権を保護するための機構について説明するための図である。

【符号の説明】

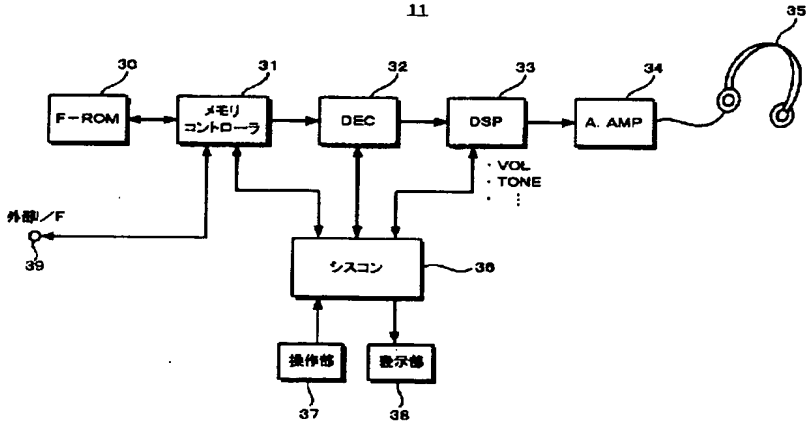
１・・・ネットワーク、２・・・クライアント、３・・・音楽配信サーバ、１０・・・パーソナルコンピュータ、１１・・・携帯用ヘッドフォンステレオ、２０・・・暗号鍵サーバ、２１・・・認証システム、２２・・・音楽データベース、２３・・・課金システム、３０・・・フラッシュメモリ、３１・・・メモリコントローラ、３６・・・シスコン、３９・・・外部インターフェイス、５１・・・ＣＰＵ、５５・・・ハードディスク、５７・・・携帯用ヘッドフォンステレオと接続するための

インターフェイス、１００・・・公開鍵、１０１・・・　　秘密鍵

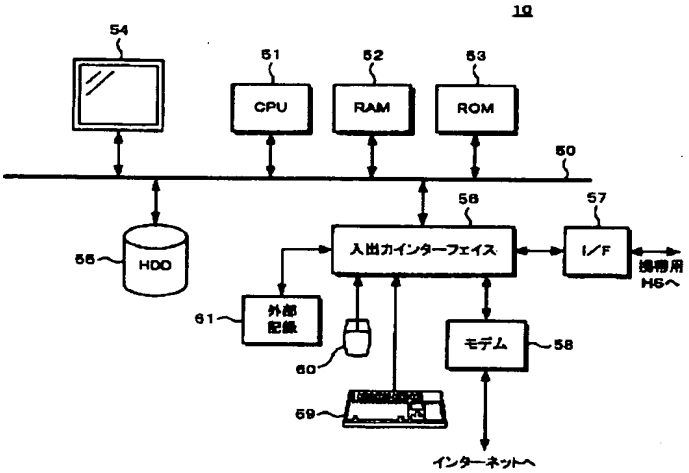
【図１】



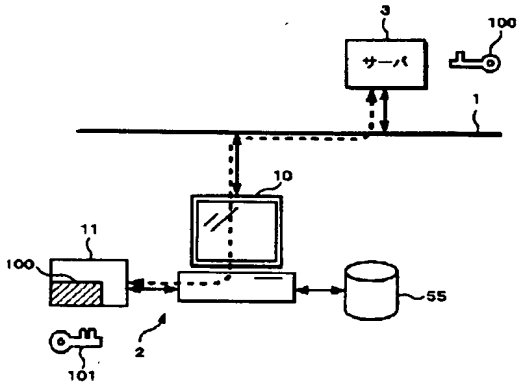
【図２】



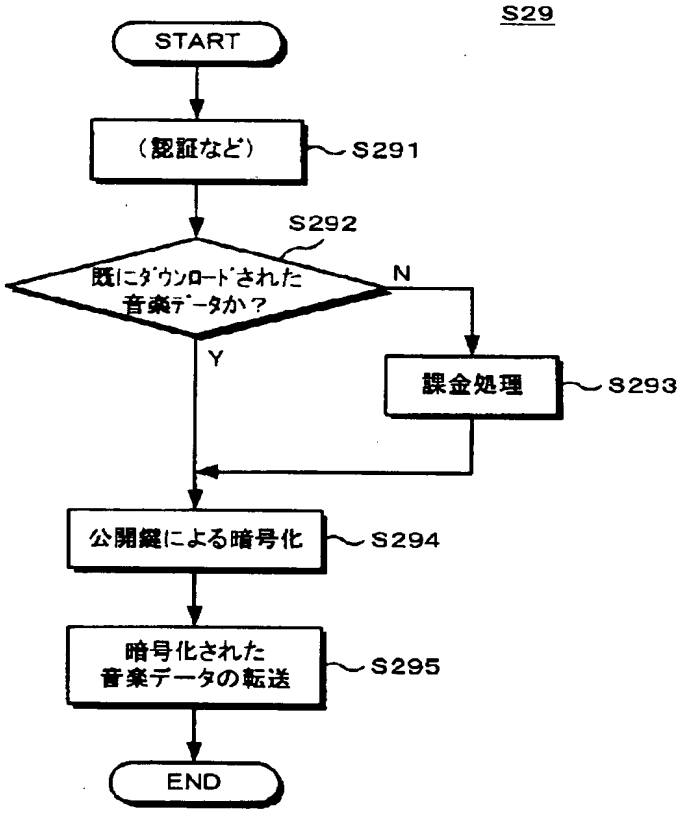
【図3】


1Q
54
51
CPU
52
RAM
53
ROM
50
55
HDD
56
入出力インターフェイス
57
I/F
携帯用
HSへ
61
外部
記憶
60
モデム
58
59
インターネットへ

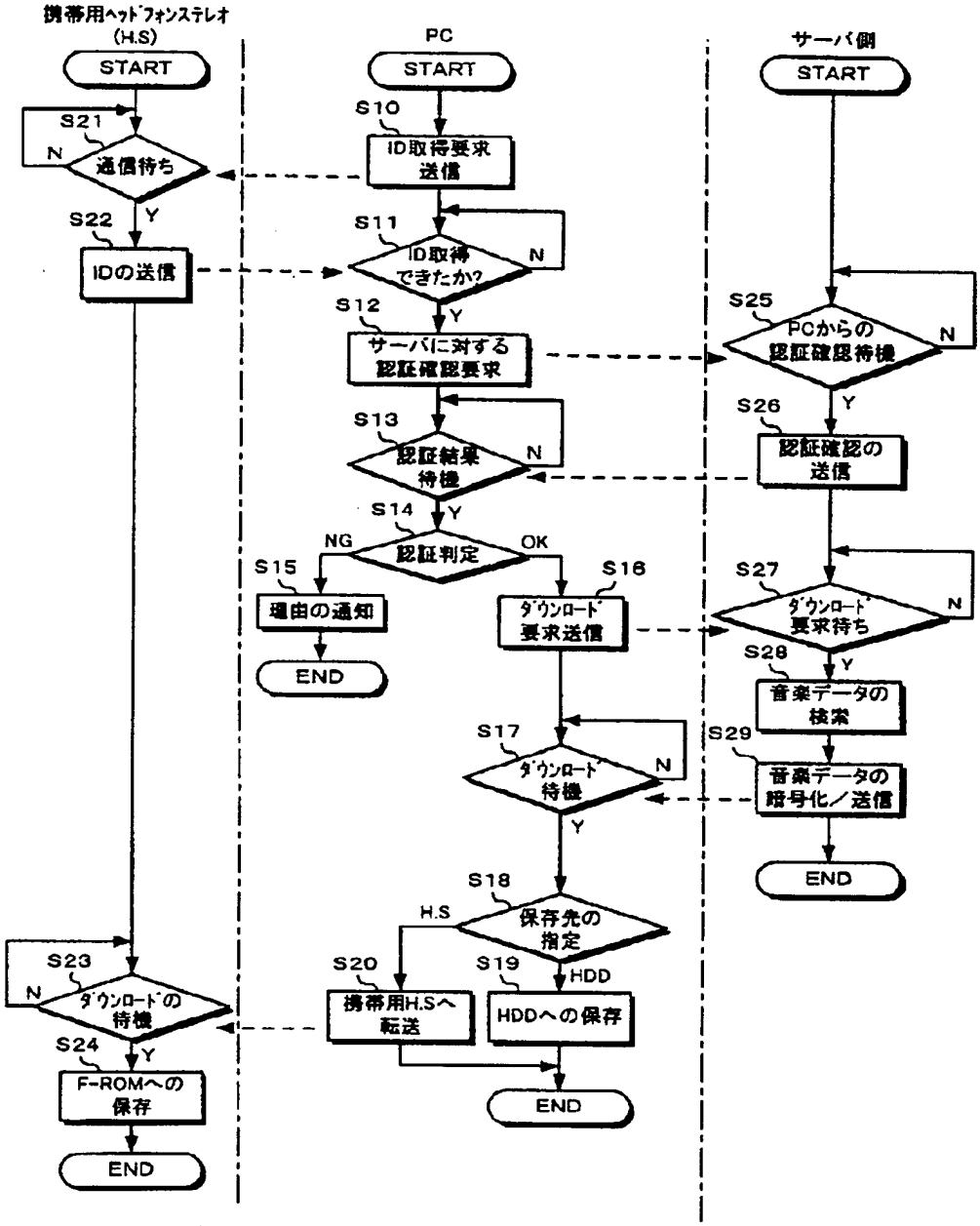
【図8】


3
サーバ
100
1
10
11
100
55
2
101

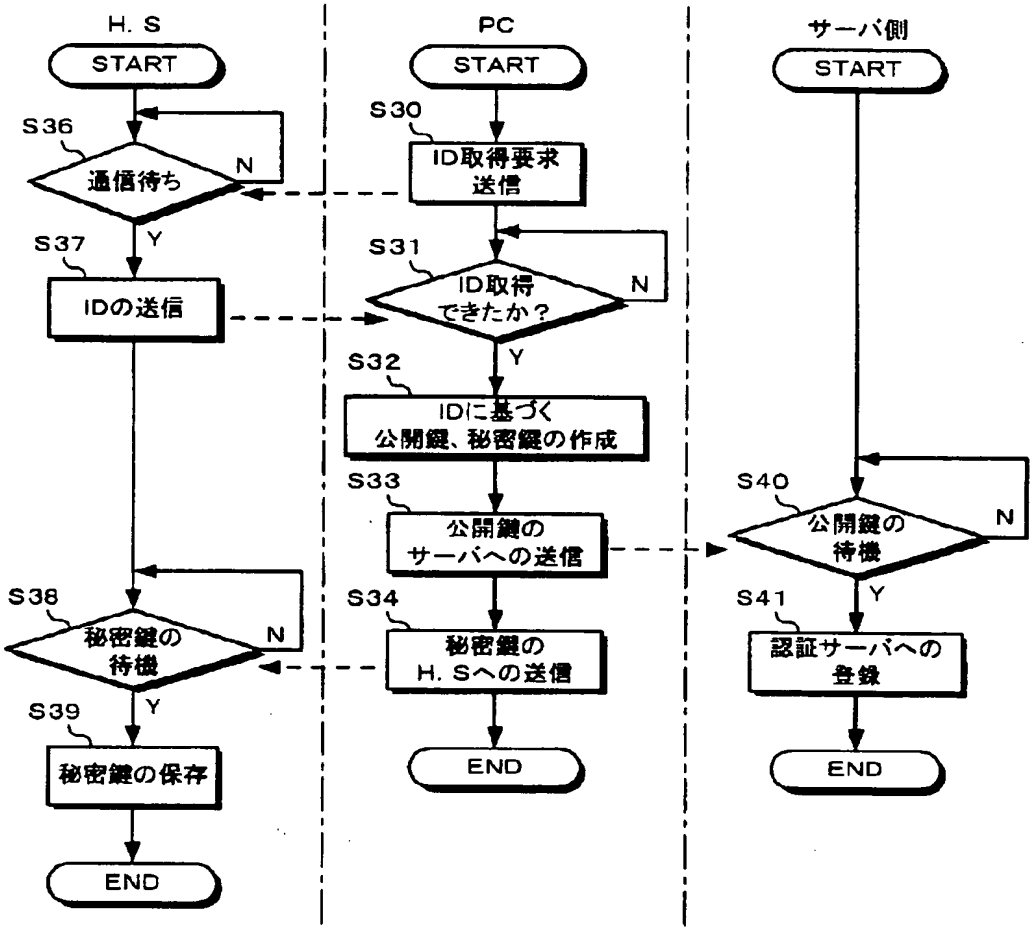
【図5】


S29
START
(認証など)
S291
S292
既にダウンロードされた
音楽データか？
N
Y
課金処理
S293
公開鍵による暗号化
S294
暗号化された
音楽データの転送
S295
END

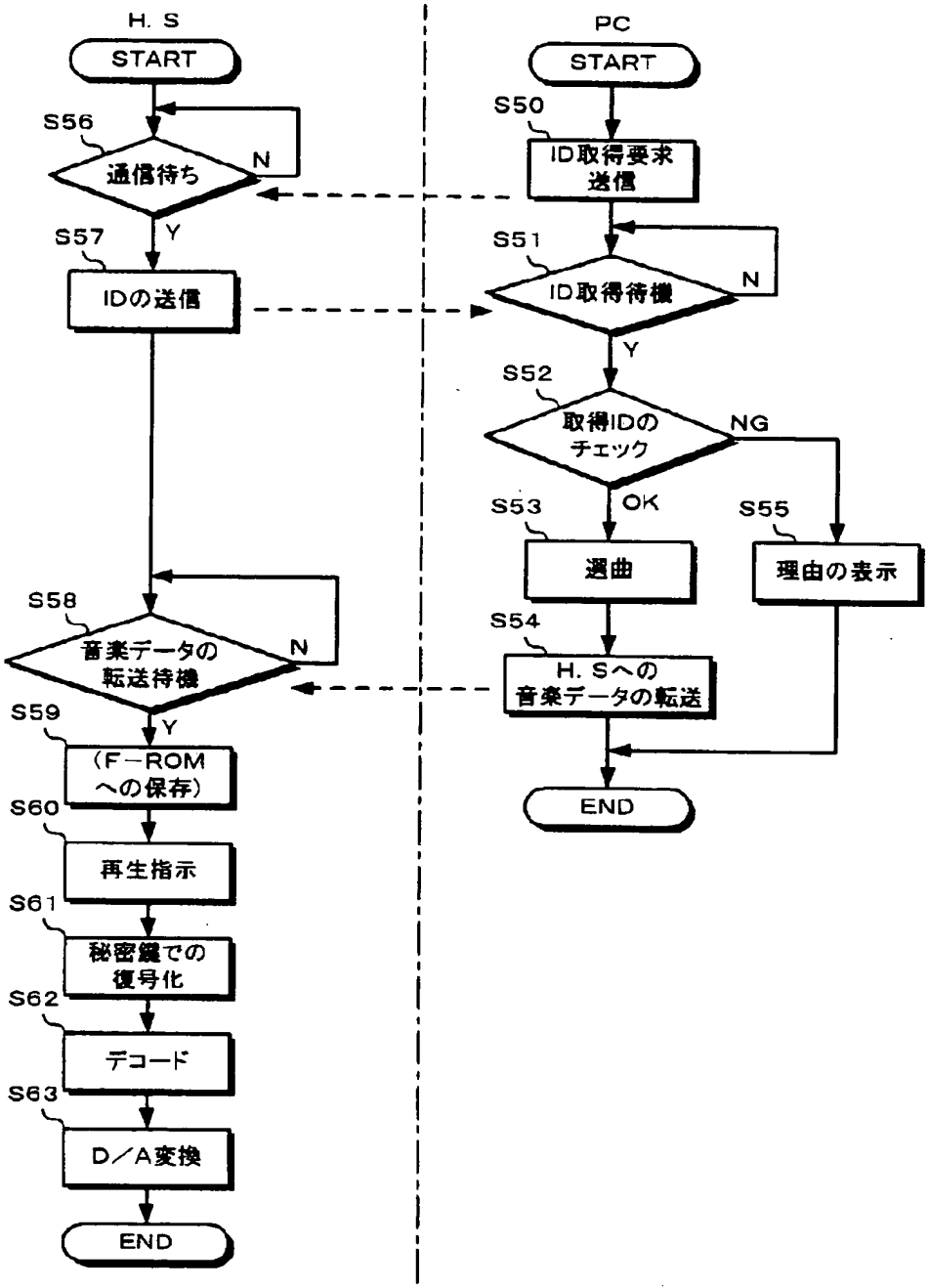
【図4】


携帯用ﾍｯﾄﾞﾌｫﾝｽﾃﾚｵ
(H.S)
START
S21
N
通信待ち
Y
S22
IDの送信
S23
N
ﾀﾞｳﾝﾛｰﾄﾞの待機
Y
S24
F-ROMへの保存
END
PC
START
S10
ID取得要求送信
S11
ID取得できたか?
N
Y
S12
サーバに対する認証確認要求
S13
認証結果待機
N
Y
S14
NG
認証判定
OK
S15
理由の通知
END
S16
ﾀﾞｳﾝﾛｰﾄﾞ要求送信
S17
ﾀﾞｳﾝﾛｰﾄﾞ待機
N
Y
S18
H.S
保存先の指定
HDD
S20
携帯用H.Sへ転送
S19
HDDへの保存
END
サーバ側
START
S25
PCからの認証確認待機
N
Y
S26
認証確認の送信
S27
ﾀﾞｳﾝﾛｰﾄﾞ要求待ち
N
Y
S28
音楽データの検索
S29
音楽データの暗号化／送信
END

【図6】


H. S
START
S36
通信待ち
N
Y
S37
IDの送信
S38
秘密鍵の待機
N
Y
S39
秘密鍵の保存
END
PC
START
S30
ID取得要求送信
S31
ID取得できたか？
N
Y
S32
IDに基づく公開鍵、秘密鍵の作成
S33
公開鍵のサーバへの送信
S34
秘密鍵のH. Sへの送信
END
サーバ側
START
S40
公開鍵の待機
N
Y
S41
認証サーバへの登録
END

【図7】


H. S
START
S56
通信待ち
N
Y
S57
IDの送信
S58
音楽データの
転送待機
N
Y
S59
(F-ROM
への保存)
S60
再生指示
S61
秘密鍵での
復号化
S62
デコード
S63
D/A変換
END
PC
START
S50
ID取得要求
送信
S51
ID取得待機
N
Y
S52
取得IDの
チェック
NG
OK
S53
選曲
S55
理由の表示
S54
H. Sへの
音楽データの転送
END

フロントページの続き

Fターム(参考) 5B089 AA16 AA22 AB01 AC03 AD06
AE09 CE08 DD03 DD06 DD07
5D108 BA04 BA06 BC01 BF11 BF12
BF13 BF20 BH10
5K101 KK18 MM07 NN03 NN18 NN21
NN48 TT06 UU16 UU19 UU20
VV06